DATE(S) ISSUED:
6/10/2010

SUBJECT:
Multiple Vulnerabilities in Microsoft Windows Help and Support Center Could Allow Remote Code Execution

OVERVIEW:
Two vulnerabilities have been identified in Microsoft Windows Help and Support Center that could allow an attacker to take complete control of an affected system. The Help and Support Center is a feature in Windows that provides help on a variety of topics. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of these vulnerabilities. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Please note: Proof of concept code has been published and is publically available. However, we have not received any reports of active exploitation of these vulnerabilities. We have tested this code in our lab and confirmed that the exploit allows for remote code execution.

At this point in time, no patches are available for these vulnerabilities.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Two vulnerabilities have been identified in Microsoft Windows Help and Support Center that could allow an attacker to take complete control of an affected system. The Help and Support Center is a feature in Windows that provides help on a variety of topics.

The first vulnerability is due to a design error in the trusted document whitelist functionality used by the Help and Support Center in Windows. The whitelist functionality restricts untrusted sites from accessing arbitrary help documents by running Help and Support Center in a restricted mode where only white listed help documents and parameters are accessible. Successful exploitation can allow attackers to bypass the whitelist functionality and access arbitrary help documents.

The second vulnerability is a cross site scripting vulnerability in the Help and Support Center application. Cross-site scripting occurs when an attacker uses a web application to send unauthorized code to an end user. This vulnerability is due to the way the Help and Support Center application fails to sanitize user-supplied input to the 'svr' parameter of the 'sysinfo/sysinfomain.htm' script. When this vulnerability is combined with the first vulnerability it could allow an attacker to execute arbitrary code on a vulnerable system.

Successful exploitation of these vulnerabilities could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

At this point in time, no patches are available for these vulnerabilities.

Please note: Proof of concept code has been published and is publically available. However, we have not received any reports of active exploitation of these vulnerabilities. We have tested this code in our lab and confirmed that the exploit allows for remote code execution.

RECOMMENDATIONS:
The following actions should be taken:
- Install the appropriate Microsoft patch as soon as it becomes available after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- If users do not rely on the protocol handler for Help and Support Center, organizations should consider disabling it by removing the following key from the registry to block the attacks: 'HKEY_CLASSES_ROOT\HCP\shell\open\command'

REFERENCES:
Security Focus:
http://www.securityfocus.com/bid/40721
http://www.securityfocus.com/bid/40725

Full Disclosure:
http://archives.neohapsis.com/archives/fulldisclosure/2010-06/0197.html